Action, inaction, trust and the common property problem of cyber security

Karen Elliott[a], Fabio Massacci[b,*], Julian Williams[a,*]

[a] *Durham University Business School, Durham, DH1 3LB, UK.*
[b] *Dipartimento di Scienze ed Ingegneria dell'Informazione, University of Trento, Via Sommarive 14, I-38123 Trento, Italy.*

Abstract

Cyber-security tends to be viewed as a highly dynamic continually evolving technology race between attacker and defender. However, economic theory suggests that in many cases doing 'nothing' is the optimal strategy when substantial fixed adjustments costs are present. Indeed, anecdotal experience off chief information security officers by the authors indicates that uncertain costs that might be incurred by rapid adoption of security updates does induce substantial delay, so the industry does appear to understand this aspect of economics quite well. From a policy perspective the inherently discontinuous adjustment path taken by firms can cause difficulties in determining a) the most effective public policy remit and b) assessing the effectiveness of any enacted policies ex-post. This article provides a short summary of the key ideas of the pressing policy issues on the cyber security agenda.

Keywords: Cyber security, return on security investment, fixed adjustment costs, real option value of delay, the public good aspect of security
JEL Classification: L14, L23, M10, M14

*Corresponding. The authors gratefully acknowledge the support of the UK Technology Strategy Board grants "Cloud Stewardship Economics", "Trust Economics" and the European Commission Seventh Framework Programme for Research and Technological Development (FP7) project "SECONOMICS" grant agreement 285223.

Email addresses: karen.elliott@durham.ac.uk (Karen Elliott), fabio.massacci@unitn.it (Fabio Massacci), julian.williams@durham.ac.uk (Julian Williams)

"You have only to rest in inaction and things will transform themselves." Chap 11 ("Let it be, leave it alone"),

Page 122. The Complete Works of Chuang Tzu. By Zhuangzi, Burton Watson, Columbia College.

1. Inaction, Decision Making and Fixed Costs

The point that inaction is sometimes the optimal path is well taken by economists. Nancy Stokey introduces her substantial volume on the topic of optimal control with: *"In situations where action entails a fixed cost, optimal policies involve doing nothing most of the time and exercising control only occasionally. . . "*,[1]. Much of the extant literature on information security focuses on the details of how cyber security threats occur and the best strategies to resolve them. Furthermore, media reporting of cyber security events in firms often key in on perceived short sighted investment strategies in the cyber security domain. Indeed, Chief information security officers (CISOs) typically ask (a) how do we measure our return on security investment and (b) on a cost-benefit basis how do I know when to patch/fix/shut-down systems when new vulnerabilities arise? Both of these questions are very difficult to answer.

Let us consider (a) momentarily. The constantly evolving state of the 'market for attacks', is part of the reason that determining the true value of security investment is so difficult. The senior corporate officer of a firm has no way of knowing empirically with a high level of confidence, if the reason the firm has had no security incidents is because: 1) the firm is spending exactly the right amount on security; 2) the firm is spending ten times more than they need or 3) that they are spending too little, but no attacker has either stumbled across their vulnerabilities or not found it worthwhile to exploit them. This lack of quantitative support for investment choices is hard to square against the typical activities of a firm in managing costs and risks. Large firms actively manage interest rate and foreign exchange risk through their treasury management functions. These activities are carefully accounted for in corporate reports alongside their normal operational activities. Hence the perceived difficulty of CISOs in protecting their budgets and the concern that after a significant event, it will be their 'successor' who will be spending the new found riches bestowed on the firms security after the horse has bolted.

In contrast, the decision to invest in a fix or a control appears to have become relatively well understood, for large technology companies at least. The algorithm is roughly as follows: 1) determine the severity of the security flaw and the level of impact on the organization, possibly using the common vulnerability scoring system (CVSS) calculator provided by the US National Institute of Standard in Technology. 2) determine the danger of implementing the patch,

[1]Nancy L Stokey. *The Economics of Inaction: Stochastic Control models with fixed costs.* Princeton University Press, 2008, Page 1:1.

how much testing is required to ensure that the patch is not as destructive as the threat. 3) weigh the first two steps up and then triage the update to either an immediate implementation or to some regular update cycle (the third Sunday of each month seems popular with several technology companies and financial institutions we have spoken to in the UK). In part[2] attempts to answer this question by posing a quantitative trade-off between the increasing risk of doing nothing and the deterministic cost associated with potentially incomplete mitigation.

Indeed, the second step in this procedure is an archetypal fixed adjustment cost in a security setting and part of the objective is to provide a consistent treatment of this problem. However, is the delay in implementation of security investment controls a catastrophic miss-step by management in not providing the resources to under-funded information security departments or simply a sensible trade-off between risk and investment? Curiously, many current economic models suggest that we maybe drifting more to the former than the latter and not because the 'suits' upstairs are taking unreasonable risks, but because of an older, much more formidable foe: the tiny invisible adjustments that drive us to the Nash equilibrium choices we make everyday as we strategize our actions and respond to the actions of others.

2. What is generating the risks?

It might seem somewhat obvious at this juncture to talk about the adversarial nature of the security problem. Moreover, understanding that the agent working against you and your peer group is an economic actor with preferences (albeit random ones) is a critically important point. So who are the attackers and what do we know about them? If we look at the prior security investment literature[3], standard treatments of the attacker view them as essentially random number generators. This treatment considers a set of vulnerabilities in commonly used software, firmware and hardware and then throws malicious agents at this set. Eventually, a combination of technical proficiency and vulnerability come together to create a tool that can genuinely threaten the economic and physical well-being of the pool of targets. As a first pass of the problem, this is a good starting point. However, it does not account for certain stylized facts that we currently observe in the hacking and security communities. First, the UN estimates that global annual GDP is estimated to be between

[2] Christos Ioannidis, David Pym, and Julian Williams. "Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach". English. In: *Economics of Information Security and Privacy III*. ed. by Bruce Schneier. Springer New York, 2013, pp. 171–191. ISBN: 978-1-4614-1980-8. DOI: 10.1007/978-1-4614-1981-5_8. URL: http://dx.doi.org/10.1007/978-1-4614-1981-5_8.

[3] L.A. Gordon and M.P. Loeb. "The Economics of Information Security Investment". In: *ACM Transactions on Information and Systems Security* 5.4 (2002), pp. 438–457; Marc Lelarge. "Coordination in Network Security Games: a Monotone Comparative Statics Approach". In: *CoRR* abs/1208.3994 (2012). URL: http://arxiv.org/abs/1208.3994.

$60 and $80 Trillion in 2014. The Brookings institute estimates that the cyber security industry accounts for approximately $77 billion (so possibly less than 1/10 of one percent) compared to conventional security expenditure on defence equipment and physical security which is around 4% of GDP at just under $400 billion. However, in a research project carried out by the authors a snapshot of transactions on a Russian online 'hacker-market', which Google and the FBI have indicated accounts for a majority of online deployed malware tools indicates that transaction sizes are quite low, often in the hundreds of dollars and only rarely in the tens of thousands.

If we look at insurance claims against cyber attacks from industry surveys, the claims from US firms are similarly very small, indeed, in the 2011 to 2013 period the median claim was $750,000 and the high was $13.5 million; this individual claim represented about 10% of the total.[4] So what do we take from this? Either we are extremely risk averse (which may be the case as reputational damage is persistent) or firms are not communicating the anticipated full costs of an attack. A further interesting puzzle comes from the research study undertaken by[5] who document the menus of vulnerabilities used by hackers in their malware kits. They conjecture that attackers are quite 'lazy'. Instead of actioning vulnerabilities in pure rank order of effectiveness in their tools, the costly effort needed to develop new tools results in them persisting with malware based on vulnerabilities long after effective patches are widely available and the apparently most profitable opportunities have been lost. Fixed costs appear to make hacker investments in exploiting vulnerabilities as similarly 'lumpy' as those of targets.

Another important point about cyber attackers is in regard to their psychological profile and self perception in terms of criminality. The importance of the differential in psychology instantiates itself in the decision of a software engineer to use deploy their labour for legal productive efforts or those deemed to be 'illegal'. Hackers appear to be able to switch relatively easily and this complicates assessment of the potential for new attacks given different innovations (for instance the failure of a widely used encryption system increasing the opportunity set).

Criminologists, see[6] for a relatively mainstream discussion commonly refer to the concept of 'consistency' in behavior. Once a pattern of offending is established it is highly likely that this pattern will persist, both in terms of their specific criminal behavior and in their wider lives. The evidence presented indicates that cyber-criminals are less easily defined by the criminal aspects of their lives than, for instance, a persistent perpetrator of grand larceny or a violent offender. Indeed, it is quite likely that they interchange between

[4] See the 'Net Diligence' survey of cyber insurance claims at `http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf`.

[5] Luca Allodi and Fabio Massacci. "The Work-Averse Attacker Model". In: *2015 European Conference on Information Systems*. ECIS. 2015.

[6] Bill McCarthy. "New economics of sociological criminology". In: *Annual Review of Sociology* (2002), pp. 417–442.

legitimate and criminal activities as any normal contract engineer would switch between topics as opportunities arise. Therefore, the pool of threats that we face is quite uncertain, if their fixed costs change, we could see sudden and dramatic increases or decreases in attacking intensity, with very little systematic methods of predicting these changes.

So we can see that the industrial organization of security investment is a complex problem. Partly, the issue lies in the design of the contract for security managers, as a buffer to adverse shocks to higher decision making teams in the firm and more importantly, the difficulty in overcoming the degree of asymmetric information between the specialist security manager and the general management of the firm. Returning back to our treasury management comparison, communicating the objectives and outcomes of the treasury management of firms has taken many hundreds of years to evolve. Likewise, the financial turmoil of 2008/9 indicates that senior managers and shareholders have not fully inculcated with the finer points of this aspect of firm performance and there is no real expectation that security, and cyber in particular, as a risk management problem will be any easier for management and shareholders to understand. Hence, a trust gap will exist: "are the cyber security experts I employ really adhering to the risk appetite of the firm, or are they simply protecting their own position?" and "are the cyber security experts using the resources I give them to efficiently protect the company or is there a lot of waste?" is indicative many comments made by senior managers and echo the kind of issues that management and financial accounting have sought to eliminate on the financing and operational side of the business. More specifically, it is partly on this issue of information asymmetry that generates some of the budgetary tension seen in large organizations, particularly when a breach has occurred and internal documents are made public.

3. Network Security, Network Externalities and the Dependency Problem

How do the micro-foundations by firm, discussed previously, aggregate to the macro and hence the public policy level? Aggregation brings certain benefits as idiosyncratic impacts from events on single firms even themselves out; however, a public policy mandate on security policy needs to be implemented at the micro-level and inappropriately onerous requirements could generate costs for the productive side of the economy and unwarranted rents other parts. For instance[7] run a simulation in which a firm that acts as a security vendor supplies of security and an insurer protecting against claims. Naturally, it can extract a quite considerable rent.

We now run into a jargon log-jam between computing science and economics as we begin to push the relative limits of meaning of the word 'network'. In an

[7]Ranjan Pal et al. "On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer". In: *IFIP Networking Conference, 2013*. IEEE. 2013, pp. 1–9.

information systems viewpoint a network is the series of nodes that exchange information vital to the operation of the organization. Economists have a quite abstract notion of a network and a sometimes slightly fuzzy interpretation of the links within a network. From the point of view of interdependent security[8] we view a network as a mechanism that adjusts the probabilistic outcomes for the various nodes. The recent work of[9] and[10] have looked at optimal decision making (in an abstract setting) when agents are arranged in fixed networks, when an individual agents (acting as a node) actions affect the costs of others. Similarly to the single firm decision making example we outlined previously and the empirical evidence on the lazy attacker the impact of fixed adjustment costs is considerable within the network.

One of the key results in game theory is the principle of 'supermodularity'. A classic treatment on supermodular games and their extensive use in public economics and industrial organisation is[11], a supermodular function is a function of two or more variables, where the joint change in gradient is strictly positive, hence players actions are reinforced. More recent work on the economic implications of network dependencies and security maybe found in[12], who apply supermodular pay-offs to network games. The resulting interpretation is that: 'If I increase my effort in an activity and it has a positive spill-over to you (like I invest in more security and discourage, by a small amount the aggregate number of attackers, whilst also reducing my own risk) then all agents within a network engage in this virtuous cycle until a Nash equilibrium is reached, although this still may not be as desirable as a coordinated action mediated by a policy maker.' However, as we ramp up fixed costs, such as the risks associated with actual act of patching the vulnerable components of your 'information network' then the firms in your economic network suffer through the interdependency in security as you forestall or neglect investments at critical points. Therefore security has a 'common property' element across firms.

We can predict that this 'lumpy' investment profile being reflected in the security interdependencies with other firms; more importantly, the lumpy profile of a very important firm can be felt across the network either directly or indirectly. Indeed, this observation formed the basis of some of the early re-

[8] See (Howard Kunreuther and Geoffrey Heal. "Interdependent Security". In: *The Journal of Risk and Uncertainty* 26.1 [2003], pp. 231–249) for a classic description of the interdependency problem in security.

[9] Yann Bramoullé, Rachel Kranton, and Martin D'Amours. "Strategic Interaction and Networks". In: *American Economic Review* 104.3 (2014), pp. 898–930. DOI: 10.1257/aer.104.3.898. URL: http://www.aeaweb.org/articles.php?doi=10.1257/aer.104.3.898.

[10] Nizar Allouch. "On the private provision of public goods on networks". In: *Journal of Economic Theory* 157 (2015), pp. 527 –552. ISSN: 0022-0531. DOI: http://dx.doi.org/10.1016/j.jet.2015.01.007. URL: http://www.sciencedirect.com/science/article/pii/S0022053115000095.

[11] Donald M Topkis. *Supermodularity and complementarity*. Princeton: Princeton university press, 1998.

[12] Daron Acemoglu, Azarakhsh Malekian, and Asuman Ozdaglar. *Network security and contagion*. Tech. rep. National Bureau of Economic Research, 2013.

search on the importance of liability sharing in security patch management, see for instance[13]. Hence, fixed costs appear to exaggerate already problematic issues of externalities transmitting costs between firms and forms the basis of our conjecture that sticky investment is generating excess aggregate security threats. Inherently, if an attacker can expect to make a good profit because somebody out there is unpatched, then they invest more time and effort (overcoming their own fixed costs) and once committed they may continue even if their risk waited return is not favourable (a process sometimes referred to as the sunk cost fallacy).

4. Thoughts for the future

Reducing fixed costs of investment, by building into information systems a degree of modularity and redundancy seems to be an ideal goal. Nevertheless, we believe it is unrealistic that we can have a fully flexible and tested way of continuously updating the security of business software. Is there any empirical evidence to support this conjecture? The straight answer is no, other than the fact that patching and implementing controls continues to be costly and breaches do occur in systems that have not been completely hardened to attack.

This process is often referred to as combinatorial innovation, in the Richard T. Ely lecture at the 2010 American Economic Association meetings Hal Varian[14] discussed the implications of an economy built around the multitude of emerging electronic communications networks.

The interesting aspect of looking at this article in 2015 is that it may have actually underestimated the degree of innovation on show as firms have made use of a wide variety development platforms. However, the basic building blocks of these information tools have become far more complex. A developer does not want to spend costly effort stripping out unwanted capability in the building blocks of their tools. The problem is that many of the redundant features within these building blocks, can combine with other features to unknown effect allowing an individual with harmful intent to analyze systems, discover vulnerabilities and generate unintended executions.

It may well be that the most important step forward in cyber security is the acknowledgement that if we are needing ever more complex systems to provide interesting and innovative avenues for economic development, we may need to accept that hardening them completely to attack could be very difficult. If we impose unrealistic expectations on the degree of integrity we may stifle the very innovation that we seek to encourage. Managing risks is part of our everyday existence and there are many risks that we cannot or really should not eliminate completely as the cost to drive them to zero may be far too high a price to pay to eliminate future fixed adjustment costs.

[13] Hasan Cavusoglu, Huseyin Cavusoglu, and Jun Zhang. "Security patch management: Share the burden or share the damage?" In: *Management Science* 54.4 (2008), pp. 657–670.

[14] Hal R Varian. "Computer mediated transactions". In: *The American Economic Review* (2010), pp. 1–10.